HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10004554-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Daniell, et al.	**Confirmation No.:**	1751
Application No.:	09/760,404	**Examiner:**	Zia, Syed
Filing Date:	01/12/2001	**Group Art Unit:**	2131
Title:	SYSTEM AND METHOD FOR RECOVERING A SECURITY PROFILE OF A COMPUTER SYSTEM		

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on July 20, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: 9/20/2005

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number_____ on _____

Number of pages:

Typed Name: Shana L. East

Signature: Shana L. East

Respectfully submitted,

Daniell, et al.

By _____

Jon E. Holland

Attorney/Agent for Applicant(s)
Reg. No. **41,077**

Date: **9/20/2005**

Telephone No.: **(256) 704-3900**

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of: **Daniell, et al.**			
Serial No.:	09/760,404	Art Unit:	2131
Filed:	January 12, 2001	Examiner:	Zia, Syed
For:	SYSTEM AND METHOD FOR RECOVERING A SECURITY PROFILE OF A COMPUTER SYSTEM	Docket No.:	10004554-1

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. §1.192 is submitted in support of the Notice of Appeal filed July 20, 2005, responding to the final Office Action of April 21, 2005.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Company Deposit Account No. 08-2025.

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope, with sufficient postage, addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 20231 on

9-20-05

Signature: Shana L. East

I. REAL PARTY IN INTEREST

The real party in interest of the instant application is the assignee, Hewlett-Packard Development Company, L.P.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences that will affect or be affected by a decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-22 are pending in the present application. The final Office Action of April 21, 2005, rejected claims 1-22 under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826).

IV. STATUS OF AMENDMENTS

No amendments have been made or requested since the mailing of the final Office Action. A copy of the current claims is attached hereto as Appendix A.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A computer system (*e.g.*, reference numeral 50) of some embodiments comprises memory (*e.g.*, reference numeral 18) and a security application (*e.g.*, reference numeral 52). The security application is configured to lock down resources of the computer system by modifying a machine state of the computer system in response to a request for activating an original state of a security profile for a user (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; and page 19, lines 16-23). The security application is configured to store data indicative of the

machine state in the memory (*e.g.*, page 20, lines 1-14), and the security application is configured to modify the machine state in response to a request for activating a new state of the security profile for the user (*e.g.*, page 20, line 15, through page 21, line 14). The security application is further configured to retrieve the data in response to a request for recovering the original state of the security profile and to modify the machine state based on the retrieved data thereby activating the original state of the security profile for the user (*e.g.*, page 21, line 15, through page 22, line 10).

In at least one embodiment, the security application, by activating the original state in response to the request for recovering the original state, enables the user to undo an error in defining the new state of the security profile for the user (*e.g.*, page 21, line 15, through page 22, line 10).

A computer system of some embodiments comprises memory (*e.g.*, reference numeral 18) and a security application (*e.g.*, reference numeral 52) defining a plurality of rules (*e.g.*, page 15, lines 15-16). The security application is configured to enable a user to select a set of the rules to define an original state of a security profile for a user, and the security application is configured to lock down the computer system by causing the computer system to enforce the selected set of rules in response to an activation request (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; and page 19, lines 16-23). The security application is further configured to store data indicative of the original state of the security profile (*e.g.*, page 20, lines 1-14), and the security application is configured to change the security profile for the user from the original state to a new state by changing which of the plurality of rules are enforced by the computer system based on inputs to the computer system (*e.g.*, page 20, line 15, through page 21, line 14). The security application is configured to retrieve the data in response to a user request, to automatically identify the set of rules based on the retrieved data, and to return the security profile for the user

to the original state thereby causing the computer system to enforce the identified rules in response to the user request (*e.g.*, page 21, line 15, through page 22, line 10).

A computer system of some embodiments comprises means (*e.g.*, reference numeral 18) for storing data and means (*e.g.*, reference numeral 52 and Figure 2) for locking down resources of the computer system by modifying a machine state of the computer system in response to a request for activating an original state of a security profile for a user (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; page 19, lines 16-23; and page 23, lines 13-17). The locking down means includes a means (*e.g.*, reference numeral 52 and Figure 2) for storing security profile data indicative of the machine state in the memory in response to the request for activating the original state of the security profile (*e.g.*, page 20, lines 1-14, and page 23, lines 17-22). The locking down means includes a means (*e.g.*, reference numeral 52 and Figure 2) for modifying the machine state in response to a request for activating a new state of the security profile for the user (*e.g.*, page 20, line 15, through page 21, line 14, and page 24, lines 9, through page 25, line 13). The locking down means includes a means (*e.g.*, reference numeral 52 and Figure 2) for retrieving the security profile data in response to a request for recovering the original state of the security profile and for modifying the machine state based on the retrieved data thereby activating the original state of the security profile for the user (*e.g.* page 21, line 15, through page 22, line 10, and page 25, line 14, through page 26, line 5).

A method of some embodiments locks down resources of a computer system (*e.g.*, reference numeral 50). The method comprises receiving a request for activating an original state of a security profile for a user and modifying a machine state of the computer system in response to the request for activating the original state of the security profile (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; and page 19, lines 16-23). The method comprises storing data indicative of the machine state (*e.g.*, page 20, lines 1-14). The method also comprises modifying the machine state in response to a request for activating a new state of the security

profile for the user (*e.g.*, page 20, line 15, through page 21, line 14). The method further comprises retrieving the data in response to a request for recovering the original state of the security profile and modifying the machine state based on the retrieved data in response to the request for recovering the first security profile (*e.g.*, page 21, lines 15, through page 22, line 10).

A method of some embodiments locks down resources of a computer system (*e.g.*, reference numeral 50). The method comprises defining a plurality of rules for locking down the computer system (*e.g.*, page 15, lines 15-16) and receiving an input from a user of the computer system (*e.g.*, page 16, lines 7-8). The method comprises selecting a set of the rules based on the input and causing the computer system to enforce the selected set of rules in response to an activation request (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; and page 19, lines 16-23). The method also comprises storing data identifying the selected set of rules in response to the activation request (*e.g.*, page 20, lines 1-14) and changing which of the plurality of rules are enforced by the computer system (*e.g.*, page 20, line 15, through page 21, line 14). The method further comprises detecting an operational problem caused by the changing and providing a request to change a security state of the computer system in response to the detecting (*e.g.*, page 21, line 15-22). The method comprises retrieving the data in response to the request to change the security state (*e.g.*, page 21, line 22, through page 22, line 1). The method further comprises automatically identifying the selected set of rules based on the retrieved data and causing the computer system to enforce the selected set of rules in response to the request to change the security state (*e.g.*, page 22, lines 1-10).

A computer system of some embodiments comprises memory (*e.g.*, reference numeral 18) and a security application (*e.g.*, reference numeral 52). The security application is configured to define a security profile for controlling access to at least one resource of the computer system and to activate an original state of the security profile (*e.g.*, page 15, lines 15-21; page 16, lines 7-14; and page 19, lines 16-23). The security application is configured to

store data indicative of the original state in the memory (*e.g.*, page 20, lines 1-14). The security application is further configured to activate a new state of the security profile in response to a user request (*e.g.*, page 20, line 15, through page 21, line 14) and to enable a user to undo an error in defining the new state by allowing the user to initiate activation of the original state based on the data (*e.g.*, page 21, line 15, through page 22, line 10).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-22 are rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826).

VII. ARGUMENT

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, *e.g.*, *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

Discussion of 35 U.S.C. §102 Rejections of Claims 1-12, 15-18 and 21

Claim 1 presently stands rejected in the final Office Action under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826). Claims 5, 8, and 9 comprise similar claimed limitations which are missing from *Hayes* (with respect to the outstanding 35 U.S.C. §102 rejections) as claim 1. Claims 2-4, 6, 7, 10-12, 15-18, and 21 depend from a respective one of the claims 1, 5, 8, and 9. Therefore, claim 1 is discussed below as an exemplary claim for discussion.

Claim 1 reads as follows:

> 1. A computer system comprising:
> memory; and
> ***a security application configured to lock down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user***, said security application configured to store data indicative of said machine state in said memory, ***said security application configured to modify said machine state in response to a request for activating a new state of said security profile for said user, said security application configured to retrieve said data in response to a request for recovering said original state of said security profile and to modify said machine state based on said retrieved data thereby activating said original state of said security profile for said user.*** (Emphasis added).

Applicants respectfully assert that *Hayes* fails to disclose at least the features of claim 1 highlighted hereinabove, and the 35 U.S.C. §102 rejection of claim 1, as amended, is therefore improper.

In rejecting claim 1, it is asserted in the final Office Action that:

> "As per claims 1, 8, and 9, Hayes teaches: memory (Fig. 2, element 212); and a security application configured to lock down resources of said computer system (col. 19, lines 50-55) by modifying a machine state of said computer system in response to a request for activating an original security profile for a user, said security application configured to store data indicative of said machine state in said memory (col. 17. lines 60-64), said security application configured to modify said machine state (col. 20, lines 1-5) in response to a request for activating a new state of said security profile *for said user* (col. 12, lines 34-46, col. 7, lines 62-63), said security application configured to retrieve said data in response to a request for recovering said original state of said security profile and to modify said machine state based on said retrieved *data thereby activating said original state of said security profile for said user* (col. 7, lines 67 col. 8, lines 5)." (Emphasis in original).

Thus, the final Office Action appears to allege that the "user applet preferences" stored at the server 202 of *Hayes* constitute the "security profiles" recited in claim 1. Applicants observe, however, that each set of "user applet preferences" or, in other words, each alleged "security profile" appears to be configured for a particular user or set of users. Thus, when a context switch occurs, a new set of "user applet preferences" is retrieved, but this new set of "user

applet preferences" appears to be configured for a different user or set of users as compared to the previously displayed set of "user applet preferences."

Claim 1 recites "modifying a machine state of said computer system in response to a request for activating an original state of a ***security profile for a user,***" further modifying the machine state in response to a request for activating a "new state" of the ***same*** "security profile" for the ***same*** "user," and activating the "original state" in response to a "request for recovering said original state of said security profile." (Emphasis added). Noting that different sets of "user applet preferences" in *Hayes* appear to be configured for different users, as described above, Applicants assert that the performance of a context switch in *Hayes* does not anticipate at least the foregoing features of claim 1.

In maintaining the rejection of claim 1, it is asserted in the final Office Action that *Hayes* teaches "a request for activating a new state of said security profile *for said user*" at column 7, lines 62-63, (emphasis in original). Such a section of *Hayes* indicates that users with "administrative authority" may "switch contexts." Such a context switch apparently retrieves a new set of "user applet preferences" so that a system administrator may make changes to the new set of "user applet preferences." See column 12, lines 36-44. Thus, it is apparently alleged in the final Office Action that "user applet preferences" or alleged "security profiles" retrieved and displayed to the system administrator before and after a context switch are both "for" the system administrator, who then constitutes the same "user" recited by claim 1.

However, there is nothing in *Hayes* to indicate that the sets of "user applet preferences" changed by the system administrator both before and after a context switch are to be used for controlling the operation of the system for the system administrator. Instead, it appears that at least one of the sets of preferences is displayed to the system administrator so he or she can change the preferences for ***other*** users. Accordingly, there is nothing in *Hayes* to indicate that the set of "user applet preferences" being changed by the system administrator before a context

switch ***and*** the set of user "user applet preferences" being changed by the system administrator after the context switch are applied to or "for" the ***same user***, including the system administrator who is making the changes. Thus, such sets of "user applet preferences" in *Hayes* cannot represent different "states" of the same "security profile" for the same "user," as described by claim 1.

In addition, as described above, a context switch appears to cause the retrieval and display of a new set of "user applet preferences" so that a system administrator may make changes to the preferences for a different user or set of users. However, there is nothing in *Hayes* to indicate that the retrieved set of "user applet preferences" is "activated" in response to the context switch. "Claims must be read in view of the specification, of which they are a part," *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979, 34 U.S.P.Q.2d 1321 (Fed. Cir. 1995), and in the instant application, a "security profile" is "activated" when a computer system begins to enforce the "security profile." See page 10, lines 15-20. There is nothing in *Hayes* to indicate that a context switch actually changes whether a set of "user applet preferences" is being enforced. Instead, it appears that a context switch presents information to a system administrator so that the system administrator may later decide whether any such preferences should be changed. Thus, a request for a context switch in *Hayes* does not constitute a "request for ***activating*** an original state of a security profile," as described by claim 1. (Emphasis added).

For at least the above reasons, Applicants respectfully assert that *Hayes* fails to disclose each feature of claim 1, as amended, and the 35 U.S.C. §102 rejection of claim 1 should, therefore, be overruled.

Discussion of 35 U.S.C. §102 Rejections of Claims 13, 14, and 20

Claim 13 presently stands rejected in the final Office Action under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826). Claim 20 comprises similar claimed limitations which are missing from *Hayes* (with respect to the outstanding 35 U.S.C. §102 rejections) as claim 13. Claim 14 depends from claim 13. Therefore, claim 13 is discussed below as an exemplary claim for discussion.

Claim 13 reads as follows:

> 13. A method for locking down resources of a computer system, comprising:
> defining a plurality of rules for locking down said computer system;
> receiving an input from a user of said computer system;
> selecting a set of said rules based on said input;
> causing said computer system to enforce said selected set of rules in response to an activation request;
> storing data identifying said selected set of rules in response to said activation request;
> changing which of said plurality of rules are enforced by said computer system;
> ***detecting an operational problem caused by said changing;***
> ***providing a request to change a security state of said computer system in response to said detecting;***
> ***retrieving said data in response to said request to change said security state;***
> ***automatically identifying said selected set of rules based on said retrieved data; and***
> ***causing said computer system to enforce said selected set of rules in response to said request to change said security state.*** (Emphasis added).

Applicants respectfully assert that *Hayes* fails to disclose at least the above features of claim 13 highlighted above. Therefore, the 35 U.S.C. §102 rejection of claim 13 is improper.

As set forth above in the Discussion of 35 U.S.C. §102 Rejections of Claims 1-12, 15-18, and 21, it is apparently alleged in the final Office Action that a context switch in *Hayes* constitutes an activation of a different "state" of a "security profile." However, there is nothing in *Hayes* to indicate that a context switch is performed in response to a detection of an "operational problem" or that any request for changing from one state of an alleged "security

profile" to another state is provided in response to an "operational problem." Thus, Applicants respectfully assert that *Hayes* fails to disclose at least the features of claim 13 highlighted above.

In maintaining the rejection of claim 13, it is asserted in the final Office Action that:

> "Regarding Claims 1-22 applicants argued that the cited prior art (CPA) [Hayes (U.S. Patent 6,339,826)] does not teach, 'a context switch is performed in response to a detection of an operational problem or that any request for changing from one state of alleged security profile to another is provided in response to an operational problem.' This is not found persuasive. Cited prior art clearly teaches system and method for a list of applications to which the user has access permission, and objects corresponding to each application in the list are downloaded. The objects when selected by the user, a request for downloading corresponding application to the user station are outputted to server. Lon-on request including user identifier is received at the server from a user station. The server uses the users log-on identifier to build a list of applications for which the user has access permission. Therefore, the system of prior art provides common repository for configuration information for users and applets in client-server environment. Allows user to login from any computer in the system at any time and have it configured automatically at run time according to *preferences* stored for the user at the server. Prevents user from winding up with applications configured on desktop to which user does not have access by *testing each application access preference* set by user against the application permission present on server. As a result, the system of cited prior art provides a system and method for automatically implementing a security profile that has been previously implemented within the computer system.

Even if the above assertions are assumed *arguendo* to be true, such assertions still fail to establish that *Hayes* discloses all features of claim 13. In this regard, even if it is assumed *arguendo* that the system of *Hayes* "automatically (implements) a security profile that has been previously implemented within the computer system," as concluded by the aforementioned Office Action assertions, there is nothing in *Hayes* to indicate that any of the alleged "security profiles" are implemented in response to a detection of "an operational problem," as recited by claim 13.

For at least the above reasons, Applicants respectfully submit that the cited art fails to disclose each feature of claim 13. Thus, the 35 U.S.C. §102 rejection of claim 13 should, therefore, be overruled.

Discussion of 35 U.S.C. §102 Rejections of Claims 19 and 22

Claim 19 presently stands rejected in the final Office Action under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826). Claim 20 comprises similar claimed limitations which are missing from *Hayes* (with respect to the outstanding 35 U.S.C. §102 rejections) as claim 19. Therefore, claim 19 is discussed below as an exemplary claim for discussion.

Claim 19 reads as follows:

> 19. The system of claim 1, wherein said security application, by activating said original state in response to said request for recovering said original state, enables said user to undo an error in defining said new state of said security profile for said user.

Applicants respectfully assert that *Hayes* fails to disclose at least the above features of claim 19, and the 35 U.S.C. §102 rejection of claim 19 is, therefore, improper.

In this regard, as set forth above in the Discussion of 35 U.S.C. §102 Rejections of Claims 1-12, 15-18, and 21, it is apparently alleged in the final Office Action that a context switch in *Hayes* constitutes an activation of a different "state" of a "security profile." Thus, in rejecting claim 19, it is apparently assumed in the final Office Action that a context switch in *Hayes* constitutes a "request for recovering (an) original state" of a security profile, as described by claim 19. Further, it is alleged in the final Office Action that the features of claim 19 are specifically disclosed by *Hayes* at column 19, lines 16-26. Such a section of *Hayes* describes an "Undo button" that allows a system administrator, when making a change to an alleged "security profile," to undo the change. However, such an undoing of a change appears to be performed independently of a context switch. Thus, there is nothing in *Hayes* to indicate that a context switch "enables" a user to "undo an error in defining said new state," as described by claim 19.

Further, Applicants observe that claim 19 recites that activation of an "original state in response to said request for recovering said ***original*** state, enables said user to undo an error in defining said ***new*** state of said security profile for said user." (Emphasis added). Moreover, if a context switch in *Hayes* recovers an alleged "original state" of a "security profile," as is apparently alleged in the Office Action, then it is the "original state" that is recovered and, therefore, displayed in response to the context switch. Thus, any undoing of an error using the "Undo button" would apparently be done either on the "state" that is displayed ***before*** the context switch or on the "original" state that is recovered by the context switch. If use of the "Undo button" occurs ***before*** a context switch, then the use of the "Undo button" cannot be "enabled" by the context switch, as described by claim 19. On the other hand, if the use of the "Undo button" is performed ***after*** the context switch on the "original state" that is recovered by the context switch, then the limitations of claim 19 are not satisfied. In this regard, the use of the "Undo button" in such a case is performed on the "original state" recovered by the context switch and, in particular, not the "new state." Thus, even if the use of the "Undo button" to undo an error in *Hayes* is somehow construed to be dependent on a context switch, all limitations of claim 19 are not satisfied by the cited sections of *Hayes*.

In addition, claim 19 depends from and, therefore, includes all of the limitations of its independent claim 1. Further, as described above in the Discussion of 35 U.S.C. §103 Rejections of Claims 1-12, 15-18, and 21, *Hayes* fails to disclose all of the features of claim 1 and is, therefore inadequate for rejecting claim 19 under 35 U.S.C. §102.

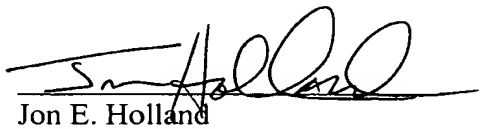
For at least the above reasons, Applicants respectfully submit that the cited art fails to disclose each feature of claim 19. Thus, the 35 U.S.C. §102 rejection of claim 19 should, therefore, be overruled.

CONCLUSION

Based on the foregoing discussion, Applicant respectfully requests that the Examiner's final rejections of claims 1-22 be overruled and withdrawn by the Board, and that the application be allowed to issue as a patent with all pending claims.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

VIII. CLAIMS - APPENDIX

1. A computer system comprising:

memory; and

a security application configured to lock down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user, said security application configured to store data indicative of said machine state in said memory, said security application configured to modify said machine state in response to a request for activating a new state of said security profile for said user, said security application configured to retrieve said data in response to a request for recovering said original state of said security profile and to modify said machine state based on said retrieved data thereby activating said original state of said security profile for said user.

2. The system of claim 1, wherein said security application includes default data defining default levels of security, wherein said security application enables a user to select one of said default levels of security, and wherein said security application is configured to modify said machine state in response to said request for activating said original state of said security profile based on said selected default level of security.

3. The system of claim 2, wherein said security application defines a plurality of rules for locking down said computer system, wherein said security application configured to enable ones of said rules based on which of said default levels is selected by said user, and wherein said security application is further configured to cause said computer system to enforce each enabled rule within said plurality of rules by modifying said machine state in response to said request for activating said original state of said security profile.

4. The system of claim 3, wherein said security application enables said user to change which of said rules are enabled.

5. A computer system, comprising:

memory; and

a security application defining a plurality of rules, said security application configured to enable a user to select a set of said rules to define an original state of a security profile for a user, said security application configured to lock down said computer system by causing said computer system to enforce said selected set of rules in response to an activation request, said security application further configured to store data indicative of said original state of said security profile, said security application configured to change said security profile for said user from said original state to a new state by changing which of said plurality of rules are enforced by said computer system based on inputs to said computer system, said security application configured to retrieve said data in response to a user request and to automatically identify said set of rules based on said retrieved data, said security application further configured to return said security profile for said user to said original state thereby causing said computer system to enforce said identified rules in response to said user request.

6. The system of claim 5, wherein said security application is further configured to define multiple sets of default data, each of said sets of default data identifying different ones of said rules as being enabled for enforcement, said security application configured to enable said user to select one of said sets of default data and to determine which of said rules are selected for inclusion into said selected set of rules based on which of said rules are indicated as enabled.

7. The system of claim 6, wherein said security application enables said user to change which of said rules are indicated as being enabled.

8. A computer system comprising:

means for storing data; and

means for locking down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user, said locking down means including a means for storing security profile data indicative of said machine state in said memory in response to said request for activating said original state of said security profile, said locking down means including a means for modifying said machine state in response to a request for activating a new state of said security profile for said user, said locking down means including a means for retrieving said security profile data in response to a request for recovering said original state of said security profile and for modifying said machine state based on said retrieved data thereby activating said original state of said security profile for said user.

9. A method for locking down resources of a computer system, comprising:

receiving a request for activating a an original state of a security profile for a user;

modifying a machine state of said computer system in response to said request for activating said original state of said security profile;

storing data indicative of said machine state;

modifying said machine state in response to a request for activating a new state of said security profile for said user;

retrieving said data in response to a request for recovering said original state of said security profile; and

modifying said machine state based on said retrieved data in response to said request for recovering said first security profile.

10. The method of claim 9, further comprising:

defining default levels of security; and

selecting one of said default levels of security,

wherein said modifying that is performed in response to said request for activating said original state of said security profile is based on said selecting.

11. The method of claim 10, further comprising:

defining a plurality of rules for locking down said computer system;

associating each of said default levels of security with different ones of said rules;

enabling ones of said rules based on which of said rules are associated, via said associating step, with said default level selected in said selecting; and

enforcing each of said rules enabled via said enabling based on said machine state as modified via said modifying that is performed in response to said request for activating said original state of said security profile.

12. The method of claim 11, further comprising:

enabling a user to change which of said rules are enabled.

13. A method for locking down resources of a computer system, comprising:

defining a plurality of rules for locking down said computer system;

receiving an input from a user of said computer system;

selecting a set of said rules based on said input;

causing said computer system to enforce said selected set of rules in response to an activation request;

storing data identifying said selected set of rules in response to said activation request;

changing which of said plurality of rules are enforced by said computer system;

detecting an operational problem caused by said changing;

providing a request to change a security state of said computer system in response to said detecting;

retrieving said data in response to said request to change said security state;

automatically identifying said selected set of rules based on said retrieved data; and

causing said computer system to enforce said selected set of rules in response to said request to change said security state.

14. The method of claim 13, further comprising:

defining multiple sets of default data, each of said sets of default data identifying different ones of said rules as being enabled; and

selecting one of said sets of default data,

wherein said selecting a set of said rules is further based on which of said sets of default data is selected via said selecting one of said sets of default data.

15. The system of claim 1, wherein said original state grants access to a particular resource of said computer system based on a user identifier, and wherein said new state denies access to said particular resource based on said user identifier.

16. The system of claim 1, further comprising an operating system configured to read said machine state modified by said security application and to control access to at least one resource of said computer system based on said machine state.

17. The computer system of claim 16, wherein said machine state read by said operating system comprises a flag indicative of whether access to said at least one resource is restricted.

18. The computer system of claim 17, wherein said operating system is configured to analyze, in response to said flag, data indicating which users are authorized to access said at least one resource.

19. The system of claim 1, wherein said security application, by activating said original state in response to said request for recovering said original state, enables said user to undo an error in defining said new state of said security profile for said user.

20. The method of claim 9, further comprising:

detecting an operational problem caused by activation of said new state of said security profile; and

providing said request for recovering said original state of said security profile in response to said detecting.

21. The method of claim 9, wherein said storing is in response to said request for activating said original state of said security profile.

22. A computer system, comprising:

memory; and

a security application configured to define a security profile for controlling access to at least one resource of said computer system, said security application configured to activate an original state of said security profile and to store data indicative of said original state in said memory, said security application further configured to activate a new state of said security profile in response to a user request, said security application further configured to enable a user to undo an error in defining said new state by allowing said user to initiate activation of said original state based on said data.

IX. EVIDENCE - APPENDIX

None.

X. RELATED PROCEEDINGS - APPENDIX

None.